

**I CLAIM:**

1. A computer program product for controlling a managing computer to manage  
5 malware protection within a computer network containing a plurality of network  
connected computers, said computer program product comprising:

receiving code operable to receive at said managing computer a plurality of  
log data messages identifying detection of malware by respective ones of said  
plurality of network connected computers;

10 detecting code operable to detect from said plurality of log data messages  
received by said managing computer a pattern of malware detection across said  
plurality of network connected computers matching one or more predetermined  
trigger patterns; and

action performing code operable in response to detection of one or more  
15 predetermined trigger patterns to perform one or more predetermined anti-malware  
actions.

2. A computer program product as claimed in claim 1, wherein said plurality of  
network connected computers each have a malware scanner that serves to scan  
20 computer files to detected malware within said computer files.

3. A computer program product as claimed in claim 2, wherein said malware  
scanner uses malware definition data to identify malware to be detected.

25 4. A computer program product as claimed in claim 3, wherein said one or more  
predetermined anti-malware actions include forcing an update of malware definition  
data being used by one or more of said plurality of network connected computers.

5. A computer program product as claimed in claim 2, wherein said one or more  
30 predetermined anti-malware actions include altering at least one scanner setting of at  
least one malware scanner such that said malware scanner performs more thorough  
malware scanning.

6. A computer program product as claimed in claim 1, wherein said one or more predetermined anti-malware actions include isolating one or more of said network connected computers from other parts of said computer network.

5 7. A computer program product as claimed in claim 1, wherein said managing computer stores said plurality of log data messages within a database.

8. A computer program product as claimed in claim 7, wherein said detecting code is operable to query said database.

10 9. A computer program product as claimed in claim 7, wherein said database includes data identifying one or more of:

malware protection mechanisms used by respective network connected computers;

15 versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

20 security settings of malware protection mechanisms used by respective network connected computers.

10. A method of managing malware protection within a computer network containing a plurality of network connected computers, said method comprising the steps of:

25 receiving at a managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers;

detecting from said plurality of log data messages received by said managing computer a pattern of malware detection across said plurality of network connected computers matching one or more predetermined trigger patterns; and

30 in response to detection of one or more predetermined trigger patterns, performing one or more predetermined anti-malware actions.

11. A method as claimed in claim 10, wherein said plurality of network connected computers each have a malware scanner that serves to scan computer files to detected malware within said computer files.

5 12. A method as claimed in claim 11, wherein said malware scanner uses malware definition data to identify malware to be detected.

13. A method as claimed in claim 12, wherein said one or more predetermined anti-malware actions include forcing an update of malware definition data being used  
10 by one or more of said plurality of network connected computers.

14. A method as claimed in claim 11, wherein said one or more predetermined anti-malware actions include altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware  
15 scanning.

15. A method as claimed in claim 10, wherein said one or more predetermined anti-malware actions include isolating one of more of said network connected computers from other parts of said computer network.  
20

16. A method as claimed in claim 10, wherein said managing computer stores said plurality of log data messages within a database.

17. A method as claimed in claim 16, wherein said detecting includes querying  
25 said database.

18. A method as claimed in claim 16, wherein said database includes data identifying one or more of:

malware protection mechanisms used by respective network connected  
30 computers;

versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

security settings of malware protection mechanisms used by respective network connected computers.

19. Apparatus for managing malware protection within a computer network  
5 containing a plurality of network connected computers, said apparatus comprising:  
receiving logic operable to receive at a managing computer a plurality of log  
data messages identifying detection of malware by respective ones of said plurality of  
network connected computers;  
detecting logic operable to detect from said plurality of log data messages  
10 received by said managing computer a pattern of malware detection across said  
plurality of network connected computers matching one or more predetermined  
trigger patterns; and  
action performing logic operable in response to detection of one or more  
predetermined trigger patterns to perform one or more predetermined anti-malware  
15 actions.

20. Apparatus as claimed in claim 19, wherein said plurality of network connected  
computers each have a malware scanner that serves to scan computer files to detected  
malware within said computer files.

21. Apparatus as claimed in claim 20, wherein said malware scanner uses malware  
definition data to identify malware to be detected.

22. Apparatus as claimed in claim 21, wherein said one or more predetermined  
25 anti-malware actions include forcing an update of malware definition data being used  
by one or more of said plurality of network connected computers.

23. Apparatus as claimed in claim 20, wherein said one or more predetermined  
anti-malware actions include altering at least one scanner setting of at least one  
30 malware scanner such that said malware scanner performs more thorough malware  
scanning.

24. Apparatus as claimed in claim 19, wherein said one or more predetermined anti-malware actions include isolating one of more of said network connected computers from other parts of said computer network.

5 25. Apparatus as claimed in claim 19, wherein said managing computer stores said plurality of log data messages within a database.

26. Apparatus as claimed in claim 25, wherein said detecting logic is operable to query said database.

10

27. Apparatus as claimed in claim 25, wherein said database includes data identifying one or more of:

malware protection mechanisms used by respective network connected computers;

15

versions of malware protection computer programs used by respective network connected computers;

versions of malware definition data used by respective network connected computers; and

20

security settings of malware protection mechanisms used by respective network connected computers.